Quadratic integral solutions to double Pell equations

Francesco Veneziano
f.veneziano@sns.it

October 4, 2011

Abstract

We study the quadratic integral points—that is, (S-)integral points defined over any extension of degree two of the base field—on a curve defined in $\mathbb{P}_3$ by a system of two Pell equations. Such points belong to three families explicitly described, or belong to a finite set whose cardinality may be explicitly bounded in terms of the base field, the equations defining the curve and the set S. We exploit the peculiar geometry of the curve to adapt the proof of a theorem of Vojta, which in this case does not apply.

1 Introduction

Let $\mathcal{C}$ be an irreducible curve defined over a number field k. We know, depending on the genus, the general structure of $\mathcal{C}(\mathbb{Q})$; on the other hand, of course $\mathcal{C}(\overline{\mathbb{Q}})$ is always infinite, so it is natural to ask what happens if we consider algebraic points up to some fixed degree over $\mathbb{Q}$.

Abramovich and Harris in [AH91], and also Silverman and Vojta in [HS91, Voj91, Voj92] were among the first to study the set of points $P \in \mathcal{C}(\overline{\mathbb{Q}})$ such that $[k(P) : k] \leq d$, in particular whether it is infinite or not.

In this paper we deal with the analogous problem for *integral* points, sticking to the special case of $d = 2$. This case was already studied in generality by Corvaja and Zannier in [CZ04, Corollary 1] using Schmidt's Subspace Theorem.

We will further specialise the problem to curves defined by a double Pell equation, such as, for example,

$$\begin{cases} y^2 = 2x^2 + 1 \\ z^2 = 3x^2 + 1. \end{cases} \tag{1}$$

Double equations of this kind are historically relevant, being among the first curves of genus 1 ever studied.[1]

Of course, by Siegel's theorem on integral points on curves, there are only finitely many solutions in $\mathbb{Z}$ to (1), but it may be easily seen that there are infinitely many solutions in algebraic integers of degree 2 over $\mathbb{Q}$: in fact it is classically known that each Pell equation $x^2 - dy^2 = 1$ has infinitely many

[1] See for instance [Wei07] or [Mor69] for a discussion of some classical cases.

integral solutions when d is a positive integer not a square, so one can solve the first equation to find infinitely many (x_n, y_n) such that $y_n^2 = 2x_n^2 + 1$, and then set $z_n = \pm\sqrt{3x_n^2 + 1}$; in this way we can actually find three infinite families of solutions. We will fully describe the set of quadratic integral points on these curves and give a geometrical meaning to the families just mentioned.

Going back to the general context, Abramovich and Harris conjectured that the set of $P \in \mathcal{C}(\overline{\mathbb{Q}})$ such that $[k(P) : k] \leq d$ is infinite (up to a finite extension of the basefield k) if and only if there exists some non constant morphism $\varphi : \mathcal{C} \to X$ of degree at most d, where X is either $\mathbb{P}_1$ or an elliptic curve E with $|E(k)| = \infty$.

Note that this condition is obviously sufficient; if φ is defined over k the preimage through φ of a rational point in X is a point of degree at most d in $\mathcal{C}$.

While the general conjecture was proved false by Dabarre and Fahlaoui in [DF93], Abramovich and Harris managed to prove it in some cases as, for example, when $d = 2, 3$.

The first step in their proofs was to consider the d-fold symmetric product of the curve, $\mathcal{C}^{(d)}$; this is a variety whose set of points may be identified with the set of all unordered d-tuples of points of $\mathcal{C}$. Points of degree at most d on $\mathcal{C}$ naturally correspond to k-rational points on $\mathcal{C}^{(d)}$, so the said authors could work on the variety $\mathcal{C}^{(d)}$ and apply results by Faltings after mapping $\mathcal{C}^{(d)}$ in an abelian variety. [2]

If we consider only points of degree 2 over the base field, the existence of infinitely many quadratic rational points is surely necessary to have infinitely many quadratic *integral* points, but it is not sufficient, as we shall see.

In [CZ04] Corvaja and Zannier prove a theorem on integral points on surfaces and apply it to $\mathcal{C}^{(2)}$ to get the following theorem:

Theorem 1. *Let $\tilde{\mathcal{C}}$ be a projective non-singular curve defined over a number field k, and $\mathcal{C} = \tilde{\mathcal{C}} \setminus \{Q_1, \ldots, Q_r\}$ be an open affine subset, for distinct $Q_i \in \tilde{\mathcal{C}}(k)$. Then*

1. *If $r \geq 5$ then $\mathcal{C}$ contains only finitely-many quadratic-integral points over k;*
2. *If $r = 4$ there exist finitely many rational maps $\psi : \tilde{\mathcal{C}} \to \mathbb{P}_1$ of degree 2 such that all but a finite number of the quadratic-integral points on $\mathcal{C}$ over k are sent to $\mathbb{P}_1(k)$ by at least one of these maps.*

As it happens for the structure of the k-integral points, what matters in this problem is the number of points at infinity.

2 Setting and statement

As mentioned above, this paper will study quadratic integral points on some special curves in $\mathbb{P}_3$ of genus 1 and with 4 points at infinity, defined by a double Pell-like equation; let then a, b, c, d be algebraic integers such that $abcd \neq 0$ and $ad - bc \neq 0$, and let $\mathcal{C}$ be the affine curve in $\mathbb{A}^3$ defined by

$$\begin{cases} y^2 = ax^2 + c \\ z^2 = bx^2 + d. \end{cases} \tag{2}$$

[2] For an account on this problem see [EE93].

Let $\tilde{\mathcal{C}}$ be its projective completion, defined by homogeneous equations

$$\begin{cases} Y^2 = aX^2 + cW^2 \\ Z^2 = bX^2 + dW^2. \end{cases}$$

Let us indicate with P_1, P_2, P_3, P_4 the four points at infinity of $\tilde{\mathcal{C}} \setminus \mathcal{C}$, which, in the coordinates $(X : Y : Z : W)$ are the points

$$\begin{aligned} P_1 &: (1 : \sqrt{a} : \sqrt{b} : 0) \\ P_2 &: (1 : \sqrt{a} : -\sqrt{b} : 0) \\ P_3 &: (1 : -\sqrt{a} : \sqrt{b} : 0) \\ P_4 &: (1 : -\sqrt{a} : -\sqrt{b} : 0). \end{aligned}$$

Let k be a number field containing $\sqrt{a}, \sqrt{b}, c$ and d, and let $S \subseteq \mathcal{M}_k$ a finite set of absolute values of k containing all the archimedean ones and all the primes in $cd(bc - ad)$; let s be the cardinality of S.

Theorem 2. *The set of quadratic S-integral points on $\mathcal{C}$ is the union of:*

- *Three families consisting of the preimages through the three maps $\mathcal{C} \to \mathbb{P}_1$*

$$\begin{aligned} (x, y, z) &\mapsto (x, y) \\ (x, y, z) &\mapsto (x, z) \\ (x, y, z) &\mapsto (y, z) \end{aligned}$$

  of the S-integral points of $\mathbb{P}_1$;

- *A finite set of cardinality at most $2^{2835s+3}$;*

- *A finite and effectively computable set whose cardinality is at most $3 \cdot 2^{1121(s+H-1)+1}$, where H is the class number of $\mathcal{O}_S$.*

Remark 3. The three families of quadratic points are indeed easy to spot. If for example the first of the two Pell equations defining $\mathcal{C}$ has integral solutions (x_n, y_n), then $(x_n, y_n, \pm\sqrt{bx_n^2 + d})$ are quadratic integral points on $\mathcal{C}$. Similarly if (x_n, z_n) are integral solutions to the second equation, then we have a second family $(x_n, \pm\sqrt{ax_n^2 + c}, z_n)$, and if (y_n, z_n) are integral solutions to $by_n^2 - az_n^2 = bc - ad$, we get $\left(\pm\sqrt{\frac{y_n^2 - c}{a}}, y_n, z_n\right)$ for a subsequence of (y_n, z_n).

Remark 4. We also note that this theorem allows for a bound on the number of exceptional solutions outside the three infinite families, while Theorem 1 does not.

While the Subspace theorem is not effective, there is a semi-effective version due to Evertse which provides an explicit bound for the *number* of exceptional hyperplanes; it is not possible, however, to use it in the proof of Theorem 1 to get such a bound for the quadratic integral points. This is because, in the proof of Theorem 1, the Subspace theorem is applied to a surface, and each exceptional hyperplane for the Subspace Theorem gives an exceptional curve on this surface which may contain points corresponding to quadratic integral points; but even if we can bound the number of such curves, they are not effectively computable and so it is not possible to bound the number of points on them.

Remark 5. We finally remark that we can not expect in general a bound for the finite sets of points which is uniform in the coefficients a, b, c, d; for example it is known[3] that there is a constant $C > 0$ such that for infinitely many positive integers A, the number of positive integer solutions to the equation $X^3+Y^3 = A$ exceeds $C\sqrt[3]{\log A}$.

3 Sketch of the proof

To study quadratic integral points we proceed as [AH91] and [CZ04] and consider the symmetric square of the affine curve $\mathcal{C}$, which is defined as the quotient of the product $\mathcal{C} \times \mathcal{C}$ by the involution which exchanges the couple (P, Q) with the couple (Q, P). This quotient is an irreducible surface which can be identified with the set of unordered couples of points, and the quotient map is

$$\begin{aligned} \mathcal{C} \times \mathcal{C} &\xrightarrow{\varphi} \mathcal{C}^{(2)} \\ (P, Q) &\mapsto \{P, Q\}. \end{aligned}$$

Consider a point P defined on a field of degree 2 over k, and let P' be its conjugate. Then the point $\{P, P'\}$ on $\mathcal{C}^{(2)}$ is fixed by every Galois automorphism of $\overline{\mathbb{Q}}/k$, and hence is defined over k. If furthermore P is an integral point so is the point $\{P, P'\}$. [4]

The special geometry of curves defined by double Pell equations carries to their symmetric square and allows one to study quadratic integral points directly and to give an explicit description of the maps mentioned in Theorem 1; for the proof we will mimic the proof of a theorem by Vojta ([Voj87]):

Theorem 6 (Vojta)**.** *Let V a projective, nonsingular variety over a number field k. Let r be the rank of the group of k-rational points of* $\mathrm{Pic}^0(V)$*, ρ the rank of the Néron-Severi group of V and D a divisor with at least* $\dim V + r + \rho + 1$ *distinct irreducible components, all defined over k. Then all sets of quasi-S-integral points on $V \setminus |D|$ are degenerate.*

Remark 7. This theorem has been improved later by Vojta himself, removing the assumptions on the Pic^0, in [Voj96] and also by Noguchi and Winkelmann in [NW02].

While this theorem does not apply to our case, the proof adapts well because on the curve $\mathcal{C}$ the difference of any two points at infinity is torsion in the Picard group.

The first step of the proof, following the strategy already illustrated, will be to study instead the structure of the set of integral points on the surface $\mathcal{C}^{(2)}$ obtained by taking the symmetric square of the original curve.

We will then follow the proof of Theorem 6 and build three functions α, β, γ without zeroes and poles on $\mathcal{C}^{(2)}$. These functions, up to constant factors, take integral points of the symmetric square to S-units.

We will then find a relation among α, β, γ, so that taking them as coordinates gives a map from $\mathcal{C}^{(2)}$ to the subvariety of $\mathbb{G}_m^3$ defined by this relation; it will turn out that this relation is linear.

[3] This result is essentially due to Mahler in [Mah35] and improved by Silverman in [Sil83].
[4] See, for example, [Ser88] for more on the symmetric product.

This means that the functions α, β, γ take integral points of $\mathcal{C}^{(2)}$ to solutions of the S-unit equation, which is the object of the following theorem.

Theorem 8 (Evertse, [Eve95])**.** *Let k be a number field, let S be a finite set of places of k containing all the archimedean ones, let $s = |S|$ and let $a_1, \dots, a_n \in \overline{\mathbb{Q}}^*$. Let $A'(a_1, \dots, a_n; \mathcal{O}_S^*)$ be the number of non degenerate solutions $x_1, \dots, x_n \in \mathcal{O}_S^*$ to the equation*

$$a_1 x_1 + \cdots + a_n x_n = 1, \tag{3}$$

where a solution $(x_1, \dots, x_n)$ is called degenerate *if there is a proper vanishing subsum in the left hand side of* (3)*. Then*

$$A'(a_1, \dots, a_n; \mathcal{O}_S^*) \leq 2^{35 n^4 s}.$$

Using this theorem we will then proceed to bound the number of non degenerate solutions and to examine degenerate solutions, which come from special subvarieties.

We will show that three of these special subvarieties are curves of genus 1, hence each gives only a finite number of quadratic integral points, while the other three have genus 0 and give three families of quadratic integral points.

The strategy outlined here would also work for any variety such that the difference of any two components of the divisor at infinity is torsion in the Picard group.

4 Proof Theorem 2

Three functions on $\mathcal{C}$ Let us consider the functions

$$\begin{aligned} f &= \frac{Y + \sqrt{a}X}{W} = \frac{cW}{Y - \sqrt{a}X} \\ g &= \frac{Z + \sqrt{b}X}{W} = \frac{dW}{Z - \sqrt{b}X} \\ h &= \frac{\sqrt{b}Y - \sqrt{a}Z}{W} = \frac{(bc - ad)W}{\sqrt{b}Y + \sqrt{a}Z}. \end{aligned}$$

They are functions on the curve $\mathcal{C}$ defined over k.
By explicit computation one has

$$\begin{aligned} x &= \frac{f^2 - c}{2\sqrt{a}f} = \frac{g^2 - d}{2\sqrt{b}g} \\ y &= \frac{f^2 + c}{2f} = \frac{bc - ad + h^2}{2\sqrt{b}h} \\ z &= \frac{g^2 + d}{2g} = \frac{bc - ad - h^2}{2\sqrt{a}h}, \end{aligned}$$

so we have that

$$k(f) = k(x, y), \quad k(g) = k(x, z), \quad k(h) = k(y, z),$$

and $k(\mathcal{C})$ has degree 2 over each of them.

The divisors of the three functions are

$$\begin{aligned}(f) &= P_3 + P_4 - P_1 - P_2\\ (g) &= P_2 + P_4 - P_1 - P_3\\ (h) &= P_1 + P_4 - P_2 - P_3.\end{aligned}$$

These three functions are in $k[\mathcal{C}]^*$, as we can see by their explicit expressions and the expressions for their inverses, or by observing that their divisors are supported on the points at infinity.

By direct computation using the first and then the second definition of f, g, h one immediately checks that they satisfy the linear relations

$$\sqrt{b}f - \sqrt{a}g = h \tag{4a}$$

$$\frac{c\sqrt{b}}{f} - \frac{d\sqrt{a}}{g} = h. \tag{4b}$$

Three functions on $\mathcal{C}^{(2)}$ Let us now consider the Cartesian product $\mathcal{C} \times \mathcal{C}$ given by equations

$$\begin{cases} y^2 = ax^2 + c\\ z^2 = bx^2 + d\\ y'^2 = ax'^2 + c\\ z'^2 = bx'^2 + d. \end{cases}$$

and let us indicate by f', g', h' the functions corresponding to f, g, h in the primed variables. Let $\mathcal{C}^{(2)}$ be the symmetric product of $\mathcal{C}$ obtained from $\mathcal{C} \times \mathcal{C}$ as a quotient by the action of $\mathbb{Z}/2\mathbb{Z}$ that acts swapping the two coordinates.

The ring of regular functions over $\mathcal{C}^{(2)}$ is $A = k[\mathcal{C} \times \mathcal{C}]^{\mathbb{Z}/2\mathbb{Z}}$, the subring of $k[\mathcal{C} \times \mathcal{C}]$ consisting of the functions invariant for this action, and the points of $\mathcal{C}^{(2)}$ can be thought as unordered couples of points on $\mathcal{C}$.

$$\begin{aligned}\mathcal{C} \times \mathcal{C} &\xrightarrow{\pi} \mathcal{C}^{(2)}\\ k[x, y, z, x', y', z'] &\supseteq A.\end{aligned}$$

Let us denote by π the quotient map from $\mathcal{C} \times \mathcal{C}$ to $\mathcal{C}^{(2)}$.

Let P be a quadratic integral point on $\mathcal{C}$, and let P' be its conjugate.

The pair (P, P') is a quadratic integral point on $\mathcal{C} \times \mathcal{C}$, and the unordered couple $\{P, P'\}$ is an integral point on $\mathcal{C}^{(2)}$ which is fixed by any Galois automorphism over k because any such morphism either fixes both P, P' or swaps them.

The point $\{P, P'\}$ is therefore defined over k.

Let us now define three functions

$$\begin{aligned}
\alpha = \frac{cd}{ff'gg'} &= (y-\sqrt{a}x)(y'-\sqrt{a}x')(z-\sqrt{b}x)(z'-\sqrt{b}x')/cd \\
\beta = \frac{c(bc-ad)}{ff'hh'} &= (y-\sqrt{a}x)(y'-\sqrt{a}x')(\sqrt{b}y+\sqrt{a}z)(\sqrt{b}y'+\sqrt{a}z')/c(bc-ad) \\
\gamma = \frac{d(ad-bc)}{gg'hh'} &= (z-\sqrt{b}x)(z'-\sqrt{b}x')(\sqrt{b}y+\sqrt{a}z)(\sqrt{b}y'+\sqrt{a}z')/d(ad-bc) \\
\frac{1}{\alpha} = \frac{ff'gg'}{cd} &= (y+\sqrt{a}x)(y'+\sqrt{a}x')(z+\sqrt{b}x)(z'+\sqrt{b}x')/cd \\
\frac{1}{\beta} = \frac{ff'hh'}{c(bc-ad)} &= (y+\sqrt{a}x)(y'+\sqrt{a}x')(\sqrt{b}y-\sqrt{a}z)(\sqrt{b}y'-\sqrt{a}z')/c(bc-ad) \\
\frac{1}{\gamma} = \frac{gg'hh'}{d(ad-bc)} &= (z+\sqrt{b}x)(z'+\sqrt{b}x')(\sqrt{b}y-\sqrt{a}z)(\sqrt{b}y'-\sqrt{a}z')/d(ad-bc).
\end{aligned}$$

We clearly see that they belong to $k[\mathcal{C}^{(2)}]$, and so do their inverses; the functions α, β, γ are the three regular and nonvanishing functions that we need to follow Vojta's strategy and view $\mathcal{C}^{(2)}$ as a subvariety of $\mathbb{G}_m^3$.

The functions α, β and γ are defined on a surface, so they must be algebraically dependent. Our next step is to find a relation between them.

Multiplying together equation (4a) for the primed and unprimed variables one gets

$$hh' = bff' + agg' - \sqrt{ab}(f'g + fg'); \tag{5}$$

doing the same for equation (4b) gives

$$hh' = \frac{c^2 b}{ff'} + \frac{d^2 a}{gg'} - cd\sqrt{ab}\left(\frac{1}{f'g} + \frac{1}{fg'}\right). \tag{6}$$

If we now multiply (6) by $\frac{ff'gg'}{cd}$ and subtract it from (5), after some tidying up and using the definitions for α, β, γ we obtain

$$\alpha + \beta + \gamma = 1.$$

Computing degrees From what we have said until now we have the mappings

$$\mathcal{C} \times \mathcal{C} \xrightarrow{\pi} \mathcal{C}^{(2)} \xrightarrow{(\alpha,\beta,\gamma)} H \subseteq \mathbb{G}_m^3$$

where H is the subvariety of $\mathbb{G}_m^3$ defined by $X + Y + Z = 1$.

The corresponding homomorphisms between the rings of regular functions are

$$k\left[X, Y, Z, \frac{1}{XYZ}\right] \xrightarrow[Z \mapsto 1-X-Y]{} k\left[X, Y, \frac{1}{XY(1-X-Y)}\right] \xrightarrow[\substack{X \mapsto \alpha \\ Y \mapsto \beta}]{} A \subseteq k[\mathcal{C} \times \mathcal{C}].$$

To find the degree of the map $\mathcal{C}^{(2)} \xrightarrow{(\alpha,\beta,\gamma)} H$ we must find the degree

$$[k(\mathcal{C}^{(2)}) : k(\alpha, \beta, \gamma)].$$

One finds directly that $(ff')^2 = -\frac{c^2\gamma}{\alpha\beta}$, so that $[k(ff', gg') : k(\alpha, \beta, \gamma)] = 2$, and from

$$\frac{f^2 - c}{\sqrt{a}f} = \frac{g^2 - d}{\sqrt{b}g}$$
$$\frac{(ff')^2 - cf^2}{\sqrt{a}(ff')f} = \frac{(gg')^2 - dg^2}{\sqrt{b}(gg')g}$$

follows that $[k(f, f', g, g') : k(ff', gg')] \leq 4$, so by our previous remarks we have

$$[k(\mathcal{C} \times \mathcal{C}) : k(\alpha, \beta, \gamma)] = [k(f, f', g, g') : k(\alpha, \beta, \gamma)] = \\ = [k(f, f', g, g') : k(ff', gg')] \cdot [k(ff', gg') : k(\alpha, \beta, \gamma)] \leq 8.$$

Obviously $[k(\mathcal{C} \times \mathcal{C}) : k(\mathcal{C}^{(2)})] = 2$, as there are two ordered pairs for a generic unordered couple; therefore we can conclude that the degree of the map given by α, β, γ between $\mathcal{C}^{(2)}$ and H is at most four.

If P is an S-integral point on $\mathcal{C}^{(2)}$ the values $\alpha(P), \beta(P), \gamma(P)$ will be S-integers, and so will be their inverses $\frac{1}{\alpha(P)}, \frac{1}{\beta(P)}, \frac{1}{\gamma(P)}$.

The point P will then provide a solution in $\mathcal{O}_S^*$ of the equation

$$x_1 + x_2 + x_3 = 1.$$

Non degenerate solutions Theorem 8 tells us that there are only finitely-many non degenerate solutions, and that we can bound their number. If we apply the theorem with $n = 3$ we obtain that the number of non degenerate triples $(\alpha, \beta, \gamma) \in H$ is at most $2^{35 \cdot 3^4 s} = 2^{2835s}$.

We already bounded in the previous paragraph the degree of the map (α, β, γ), which is at most four. For every integral point on $\mathcal{C}^{(2)}$ we have two quadratic integral points on $\mathcal{C}$, hence the number of quadratic integral points on $\mathcal{C}$ corresponding to non degenerate solutions is at most $2^{2835s+3}$.

Degenerate solutions The degenerate solutions to $\alpha + \beta + \gamma = 1$ are those with a subsum equal to 0, that is those for which one of the three functions α, β, γ is equal to 1; let us then define

$$W_\alpha : \alpha = 1, \qquad W_\beta : \beta = 1, \qquad W_\gamma : \gamma = 1$$

the subsets of $\mathcal{C}^{(2)}$ thus obtained.

Using the definition of α, β, γ we see that, for example,

$$\alpha = 1, \qquad \beta = -\gamma$$
$$ff'gg' = cd, \qquad \frac{c(bc - ad)}{ff'hh'} = -\frac{d(ad - bc)}{gg'hh'}$$
$$ff'\frac{cgg'}{d} = c^2, \qquad ff' = \frac{cgg'}{d}$$
$$(ff')^2 = c^2, \qquad gg' = \frac{ff'}{c}d$$

and similarly for the other two cases, so we see that $W_\alpha, W_\beta, W_\gamma$ are composed of two subvarieties each, and

$$\begin{aligned} W_\alpha &= W_x^- \cup W_x^+ \\ W_\beta &= W_y^- \cup W_y^+ \\ W_\gamma &= W_z^- \cup W_z^+, \end{aligned}$$

where

$$\begin{aligned} W_x^- &= \{ff' = c, gg' = d\} & W_x^+ &= \{ff' = -c, gg' = -d\} \\ W_y^- &= \{ff' = -c, hh' = ad - bc\} & W_y^+ &= \{ff' = c, hh' = bc - ad\} \\ W_z^- &= \{gg' = -d, hh' = bc - ad\} & W_z^+ &= \{gg' = d, hh' = da - bc\}. \end{aligned}$$

These six subvarieties give all degenerate solutions; to understand them better we use the following simple lemma:

Lemma 9. *Let $P = ((x, y, z), (x', y', z')) \in \mathcal{C} \times \mathcal{C}$. Then*

- $ff'(P) = \pm c \Rightarrow x = \mp x'$ *and* $y = \pm y'$;
- $gg'(P) = \pm d \Rightarrow x = \mp x'$ *and* $z = \pm z'$;
- $hh'(P) = \pm(bc - ad) \Rightarrow z = \mp z'$ *and* $y = \pm y'$.

Proof. For example, if $ff' = c$ then

$$x' = \frac{(f')^2 - c}{2\sqrt{a}f'} = \frac{c^2/f^2 - c}{2\sqrt{a}c/f} = \frac{c - f^2}{2\sqrt{a}f} = -x,$$

and similarly for the other five cases. □

If we define six subvarieties of $\mathcal{C} \times \mathcal{C}$

$$\begin{aligned} V_x^\pm &: x = \pm x', y = \mp y', z = \mp z' \\ V_y^\pm &: x = \mp x', y = \pm y', z = \mp z' \\ V_z^\pm &: x = \mp x', y = \mp y', z = \pm z', \end{aligned}$$

then the lemma tells us that each of them corresponds through π to the similarly named subvariety $W_{x,y,z}^\pm$ of $\mathcal{C}^{(2)}$ (we denote by $V_{x,y,z}^\pm$ any of the six varieties $V_x^-, V_x^+, V_y^-, V_y^+, V_z^-, V_z^+$, and we do the same with $W_{x,y,z}^\pm$). In short we have that

$$\pi|_{V_{x,y,z}^\pm} : V_{x,y,z}^\pm \to W_{x,y,z}^\pm$$

Note also that $V_{x,y,z}^\pm \simeq \mathcal{C}$ through the projection on the first component of $\mathcal{C} \times \mathcal{C}$, so that these six curves all have genus one.

Points on $W_{x,y,z}^+$ Consider for example

$$\begin{aligned} \pi|_{V_x^+} &: V_x^+ \to W_x^+ \\ ((x, y, z), (x, -y, -z)) &\mapsto \{(x, y, z), (x, -y, -z)\}. \end{aligned}$$

A generic point in W_x^+ has two preimages, obtained by exchanging the order of the pair; the points which have just one primage are those such that $y = z = 0$, but we see from the defining equations (2) of $\mathcal{C}$ that this can never happen because $by^2 - az^2 = bc - ad \neq 0$. The map $\pi|_{V_x^+}$ is therefore an unramified covering of W_x^+, and the Riemann-Hurwitz formula tells us that

$$\begin{aligned} 0 = 2g(V_x^+) - 2 = 2(2g(W_x^+) - 2) \\ g(W_x^+) = 1. \end{aligned}$$

The same is true for W_y^+ and W_z^+, because there is no point on $\mathcal{C}$ where two of x, y, z both vanish.

We have thus shown that the three subvarieties $W_{x,y,z}^+$ are all curves of genus 1, so they carry only a finite number of integral points, which in turn correspond to a finite number of quadratic integral points on $\mathcal{C}$.

We might also argue the finiteness of quadratic integral points coming from the curves $W_{x,y,z}^+$ as follows: let $K = k(\sqrt{\varepsilon})$ be a quadratic extension of k, we may suppose $\varepsilon \in \mathcal{O}_S$; let $P = (x_0, y_0, z_0)$ be a K-integral point on $\mathcal{C}$, and $P' = (x_0', y_0', z_0')$ its conjugate. Suppose that (P, P') belongs to V_x^+; if it is so, after enlarging S to an S' so that $\mathcal{O}_{S'}$ has trivial class group, we can write $x_0 = t, y_0 = u\sqrt{\varepsilon}, z_0 = v\sqrt{\varepsilon}$ for some $t, u, v \in \mathcal{O}_{S'}$.

Substituting back into the equations for $\mathcal{C}$ we get $b\varepsilon u^2 - a\varepsilon v^2 = bc - ad$, so ε divides $bc - ad$; different ε differing only by a square factor give the same extension, and given that $\mathcal{O}_{S'}^*/(\mathcal{O}_{S'}^*)^2$ is finite we see that K must belong to a finite set of extensions of k, whose cardinality may be bounded in terms of the cardinality of S'.

We know, by Siegel's theorem, that there are only finitely many integral points on $\mathcal{C}$ defined over a fixed number field; since $\mathcal{C}$ has four points at infinity, this number may be bounded effectively, as done in [CZ03], in terms of the degree of K and the cardinality of the extension of S' to K, which in turn are both bounded in terms of k and $|S'|$.

The computations involved in this bound are quite heavy, but again the special structure of the curve $\mathcal{C}$ provides us with a simpler argument: equation (4a) gives the unit equation

$$\frac{\sqrt{b}f}{h}(P) - \frac{\sqrt{a}g}{h}(P) = 1, \tag{7}$$

so the number of solutions may be easily bounded using again Theorem 8. For a fixed K and extension S'' of the set of absolute values S', there are at most $2^{35 \cdot 2^4 |S''|} = 2^{1120|S'|}$ solutions; the number of extensions K is at most $|\mathcal{O}_{S'}^*/(\mathcal{O}_{S'}^*)^2| = 2^{|S'|}$; the functions f/h and g/h have degree two, as we can see computing their divisors, so each solution gives at most two points. Combining all, we have that the number of quadratic integral points P such that (P, P') lies on any of the $W_{x,y,z}^+$ is at most $3 \cdot 2^{1121|S'|+1} = 3 \cdot 2^{1121(s+H-1)+1}$, where H is the class number of $\mathcal{O}_S$.

I thank the anonymous referee for suggestions about this bound.

We should also remark that, since the relevant curve has genus 1, it is in fact possible, as is well known, to bound *the height* of the solutions themselves; tha same can be done on equation (7), using effective results on *two-term* unit

equations (derived from Baker's theory of linear forms in logarithms). So the quadratic integral points arising from $W^+_{x,y,z}$ are, in fact, effectively computable (in contrast with those arising from the "non degenerate solutions").

Points on $W^-_{x,y,z}$ Reasoning as we did before, we consider, for example

$$\begin{aligned}\pi|_{V_x^-} : V_x^- &\to W_x^- \\ ((x,y,z),(-x,y,z)) &\mapsto \{(x,y,z),(-x,y,z)\}.\end{aligned}$$

This is again a map of degree 2.

In this case however, we see that it is ramified at points where $x = 0$, and there are 4 such points on $\mathcal{C}$, namely $(0, \pm\sqrt{c}, \pm\sqrt{d})$, each of them of course ramified of index 2. Therefore this time applying the Riemann-Hurwitz formula we obtain

$$\begin{aligned}0 = 2g(V_x^-) - 2 = 2(2g(W_x^- - 2) + 4 \\ g(W_x^-) = 0;\end{aligned}$$

as W_x^- has genus 0, it may contain infinitely many integral points.

The composition of the maps

$$\begin{aligned}\mathcal{C} \to V_x^- \to W_x^- \xrightarrow{\pi|_{W_x^-}} \{by^2 - az^2 = bc - ad\} \simeq \mathbb{P}_1 \\ (x,y,z) \mapsto ((x,y,z),(-x,y,z)) \mapsto \{(x,y,z),(-x,y,z)\} \mapsto (y,z)\end{aligned}$$

gives a map of degree two from $\mathcal{C}$ to $\mathbb{P}_1$ that takes quadratic integral points arising from W_x^- to integral points in $\mathbb{P}_1$; this map together with the same compositions for W_y^- and W_z^-, that is,

$$\begin{aligned}\mathcal{C} \to \{z^2 = bx^2 + d\} \simeq \mathbb{P}_1 \\ (x,y,z) \mapsto (x,z),\end{aligned}$$

and

$$\begin{aligned}\mathcal{C} \to \{y^2 = ax^2 + c\} \simeq \mathbb{P}_1 \\ (x,y,z) \mapsto (x,y),\end{aligned}$$

are the maps in Theorem 1.

Acknowledgments The author thanks Professors Corvaja, Evertse and Zannier for the substantial advice received in the preparation of this article, and the anonymous referee for the thorough report and for having suggested some improvements.

References

[AH91] D. Abramovich and J. Harris, *Abelian varieties and curves in $W_d(C)$*, Compositio Math. **78** (1991), no. 2, 227–238. MR MR1104789 (92c:14022)

[CZ03] P. Corvaja and U. Zannier, *On the number of integral points on algebraic curves*, J. Reine Angew. Math. **565** (2003), 27–42. MR MR2024644 (2004j:11059)

[CZ04] ———, *On integral points on surfaces*, Ann. of Math. (2) **160** (2004), no. 2, 705–726. MR MR2123936 (2005m:11118)

[DF93] O. Debarre and R. Fahlaoui, *Abelian varieties in $W^r_d(C)$ and points of bounded degree on algebraic curves*, Compositio Math. **88** (1993), no. 3, 235–249. MR MR1241949 (94h:14028)

[EE93] B. Edixhoven and J.-H. Evertse (eds.), *Diophantine approximation and abelian varieties*, Lecture Notes in Mathematics, vol. 1566, Springer-Verlag, Berlin, 1993, Introductory lectures, Papers from the conference held in Soesterberg, April 12–16, 1992. MR MR1288998 (95g:11061)

[Eve95] J.-H. Evertse, *The number of solutions of decomposable form equations*, Invent. Math. **122** (1995), no. 3, 559–601. MR MR1359604 (96i:11034)

[HS91] J. Harris and J. Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. **112** (1991), no. 2, 347–356. MR 1055774 (91i:11067)

[Mah35] K. Mahler, *On the lattice points on curves of genus 1*, Proc. London Math. Soc. **39** (1935), 431–466.

[Mor69] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics, Vol. 30, Academic Press, London, 1969. MR 0249355 (40 #2600)

[NW02] J. Noguchi and J. Winkelmann, *Holomorphic curves and integral points off divisors*, Math. Z. **239** (2002), no. 3, 593–610. MR 1893854 (2003b:32019)

[Ser88] J.-P. Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988, Translated from the French. MR MR918564 (88i:14041)

[Sil83] J. H. Silverman, *Integer points on curves of genus* 1, J. London Math. Soc. (2) **28** (1983), no. 1, 1–7. MR 703458 (84g:10033)

[Voj87] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, vol. 1239, Springer-Verlag, Berlin, 1987. MR MR883451 (91k:11049)

[Voj91] ———, *Arithmetic discriminants and quadratic points on curves*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 359–376. MR MR1085268 (92j:11059)

[Voj92] ———, *A generalization of theorems of Faltings and Thue-Siegel-Roth-Wirsing*, J. Amer. Math. Soc. **5** (1992), no. 4, 763–804. MR 1151542 (94a:11093)

[Voj96] ———, *Integral points on subvarieties of semiabelian varieties. I*, Invent. Math. **126** (1996), no. 1, 133–181. MR MR1408559 (98a:14034)

[Wei07] A. Weil, *Number theory*, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2007, An approach through history from Hammurapi to Legendre, Reprint of the 1984 edition. MR 2303999 (2007k:01003)